REMARKS

Status of the Claims

- Claims 1-2, and 4-13 are pending in the Application after entry of this amendment.
- Claims 1-2, and 4-13 are rejected by Examiner.
- Claims 1, and 4-7 are amended by Applicant.

Claim Rejections Pursuant to 35 U.S.C. §101

Claims 1-2 and 4-13 stand rejected under 35 U.S.C. § 101 as being unpatentable because the claims do not state a process that is tied to a particular machine. Applicant respectively traverses the rejection via amendment.

Independent Claims 1 and 5 are amended to recite a process performed by a receiver apparatus and a transmitter apparatus respectively. Both the preamble and the elements of independent Claims 1 and 5 are amended to include the respective apparatus. Dependent Claims 4 and 6-7 are amended to comport with their respective amended independent claims. This amendment is supported by the as-filed Figures and specification which indicate, in at least one non-limiting example, a transmitter apparatus (e.g. Set top Box), and a receiver apparatus (e.g. Digital Television).

Since both methods and machines (apparatuses) are explicitly patentable subject matter under 35 USC §101, then Applicant submits that the pending claims recite patentable subject matter. Applicant respectfully requests withdrawal of the 35 USC §101 rejection based on the amendments and discussion herein.

Claim Rejections Pursuant to 35 U.S.C. §103

Claims 1-2, 5, 7-8, 10, and 12-13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied

cryptography" (Menezes) in view of U.S. Patent No. 6,763,112 to Haumont (Haumont) in further view of US Patent No. 7, 234,059 to Beaver et al.(Beaver). Applicant respectively traverses the rejection.

Applicant respectfully submits that the above-stated combination of Menezes, Haumont, and Beaver does not render the pending claims obvious under 35 USC §103 because the combination renders Menezes unsatisfactory for its intended purpose and because Menezes teaches away from the current invention. The explanation follows.

Menezes at p 402, lines 1-8, discloses an example of mutual authentication using random numbers. The example includes the following, in Menezes notation:

1. B → A: r_B
2. A → B: $E_K(r_A, r_B, B^*)$
3. B → A: $E_K(r_B, r_A)$

A: decrypts (3) and A checks that both random numbers in (2) match those used earlier.

Wherein:

- B→ A represents B transmitting to A
- E_K represents a symmetric encryption algorithm with a key K shared between A and B.
- r_A and r_B are random numbers for A and B respectively
- B^* is an identifier element.

As stated in Menezes p 401, para 10.16, lines 11-13 states:

"It is assumed that both parties are aware of the claimed identity of the other, either by context, or by additional (unsecured) clear text data fields." (See Menezes, 10.16). This is further underlined by the protocol in 10.17(ii) that clearly includes the identity of the other party. Applicant concludes that

Menezes teaches a non-anonymous protocol that requires that parties are informed of the identity of the other.

Applicant notes that Menezes on page 33 defines a cryptographic protocol as a precise set of required actions. Menezes on page 33 states:

> **1.55 Definition** A *cryptographic protocol* (*protocol*) is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Furthermore, the first three lines of page 401 state:

> The apparent simplicity of the techniques presented below and in §10.3.3 is misleading. The design of such techniques is intricate and the security is brittle: those presented have been carefully selected.

Thus, being captive of established prejudices in his field, the skilled person would not wish to try to modify an established protocol such as in Menezes in order to arrive at the solution taught by the present claims, as the skill person is well aware that any modification to Menezes could render the modified system inoperable because of the intricate and brittle nature of such systems. While it may be argued that the skilled person is constantly concerned with the improvement of known devices or products, Menezes clearly states on pages 35:

> **1.62 Remark** (*protocol design*) When designing cryptographic protocols and mechanisms, the following two steps are essential:
>
> 1. identify *all* assumptions in the protocol or mechanism design; and
> 2. for each assumption, determine the effect on the security objective if that assumption is violated.

Here, it is useful to understand that one of skill in the art would recognize that breaking a required assumption of Menezes would result in the method of Menezes failing to achieve the Menezes security objective. Specifically, since Menezes specifically states in section 10.16 that both parties are aware of the claimed identity of the other in order for the method to function, then a violation

of this assumption results in the method Menezes failing to achieve the security objective of a functional authentication mechanism.

Applicant also respectfully concludes and submits that the cited method cited by Menezes requires non-anonymous operation because of the explicit requirement that the parties know of each other's identity for the method to function. Thus, the cited method of Menezes teaches away from anonymous operation as recited in the pending claims.

Haumont describe a system that provides a security procedure for use with a Universal Mobile Telephone Service (UMTS) for triggering the authentication of a Mobile Station (MS) and/or the generation of a new integrity key (IK) and/or a new ciphering key (CK) by the Core Network (CN) in response to a communication failure detected by a Radio Network Controller (RNC) of a Universal Radio Access Network (URAN). (See Haumont, co. 3, lines 35-42)

Beaver describes a method of performing electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, comprising: generating a plurality of random numbers; distributing in a digital medium the plurality of random numbers to the members of the group; publishing a hash value of contents of the digital medium; distributing to the members of the group public-key-encrypted messages each containing a same token comprising a random number; and encrypting a message with a key generated from the token and the plurality of random numbers. (see Beaver, col. 4, lines 13-24.)

As stated in the present Office Action dated 7/14/2009, on page 7:

"Beaver et al. teaches an anonymous authentication (see col. 4 lines 13 – col. 5 lines 30)". Applicant agrees. Thus, Beaver operates in an environment where the parties are anonymous whereas Menezes specifically operates under the Menezes operational assumption (a requirement for operation) that the parties are non-anonymous. As a result, Applicant respectfully concludes

that the anonymous system of Beaver cannot be combined with the non-anonymous method of Menezes without breaking the operational requirement of Menezes that the parties know the identities of the other.

Since the addition of Beaver operates such that the parties are anonymous, and the method of Menezes requires that the parties non-anonymous because they are known to each other, then the method Menezes is rendered inoperable by the addition of the anonymous operation of Beaver. Simply stated, if the parties are forced to be anonymous in Menezes, then the method of Menezes fails to function. Accordingly, one of skill in the art would not be motivated to combine the references of Menezes and Beaver because doing so would render Menezes inoperable. This common sense conclusion concerning a lack of motivation to combine references is reflected in MPEP §2143.01 Part V, Revision 7 of the Eighth Edition of the MPEP, dated July 2008, which reads as follows:

"THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE

If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." (MPEP §2143.01 Part V).

Since the combination of Menezes, Haumont, and Beaver prevents proper operation of Menezes because the anonymous operation of Beaver breaks the requirement of non-anonymous operation of Menezes, then the combination of the cited references fails to render the claimed invention obvious under 35 USC §103 because there is no suggestion or motivation to make the proposed modification per MPEP §2143.01 Part V.

In addition, as stated above, Applicant believes that Menezes teaches a non-anonymous protocol by requiring that both parties have knowledge of the other. The non-anonymous protocol of Menezes essentially teaches away from an anonymous protocol, such as described by Beaver. The pending claims represent an inventive example of an anonymous authentication protocol. Thus, Applicant concludes that the combination of any anonymous protocol,

such as described by Beaver, violates the non-anonymous requirements of Menezes, and results in the method of Menezes becoming inoperable due to the modification by Beaver.

Accordingly, Applicant respectfully submits that the combination of Menezes, Haumont, and Beaver does not form a prima facie case of obviousness under 35 USC §103 because:

(1) The Menezes non-anonymous method teaches away from the anonymous method recited in the pending claims, and

(2) The combination of Menezes and Beaver renders the method of Menezes unsatisfactory for its intended purpose per MPEP §2143.01 Part V because the autonomous method of Beaver breaks the non-anonymous assumption of Menezes that is needed for proper Menezes method operation.

Applicant respectfully requests reconsideration and withdrawal of the 35 USC §103(a) rejections on Claims 1-2, 5, 7-8, 10, and 12-13 in light of the arguments presented above.

Claims 4, 6, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" (Menezes) in view of U.S. Patent No. 6,763,112 to Haumont (Haumont), and in further view of U.S. Patent No. 5,815,665 to Teper et al. (Teper).

Applicant notes that Beaver is not included in the above combination, yet Claims 4, 6, 9, and 11 are dependent on independent Claims 1 and 5 whose 35 USC §103 rejection includes the teachings of Beaver.

The teachings of Menezes and Haumont are discussed above.

Teper discusses an Online Brokering Service provides user authentication and billing services to allow users to anonymously and securely purchase online services from Service Providers (SP) sites (e.g., World Wide Web sites) over a distributed public network, which may be an untrusted public

network such as the Internet. Users and SP sites initially register with the Brokering Service, and are provided with respective client and server software components for using the Brokering Service. In one embodiment, when a user initially connects to an SP site, the SP site transmits a challenge message over the public network to the user computer, and the user computer generates and returns and cryptographic response message (preferably generated using a password of the user). The SP site then passes the response message to the Brokering Service, which in-turn looks up the user's password and authenticates the response message. (See Teper, Abstract).

However, the addition of Teper to the combination Menezes and Haumont cannot overcome the aspect that Menezes teaches away from the claimed invention and that the anonymous operation of Teper also violates the non-anonymous operational requirement of Menezes that the parties know each other's identity. Thus, as explained above with respect to independent Claims 1 and 5, the combination of Menezes which operates in a non-anonymous manner cannot be combined with a reference, such as Teper, that teaches an anonymous operational method because it violates the common sense rule expressed in MPEP §2143.01 Part V.

As a result, Applicant respectfully submits that the combination of Menezes, Haumont, and Teper cannot render obvious independent Claims 1 and 5 and their respective dependent Claims 4, 6, 9, and 11 under 35 USC §103(a) per MPEP §2143.01 Part V and because the non-anonymous requirement of Menezes teaches away from the present invention.

Conclusion

Applicant respectfully submits that the pending claims patentably define over the cited art and respectfully requests reconsideration and withdrawal of all rejections of the pending claims. Reconsideration for a Notice of Allowance for all pending claims is respectfully requested.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 07-0832 therefore.

Respectfully submitted,

Eric Diehl et al.

Date: November 11, 2009

/Jerome G. Schaefer/
Jerome G. Schaefer
Attorney for Applicant
Registration No. 50,800
(609) 734-6451

Thomson Licensing, LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312